

(i) *North Korea*. Applications for military end-users or for military end-uses, or for nuclear end-users or nuclear end-uses, in North Korea of such equipment will generally be denied. Applications for non-military end-users or for non-military end-uses, or for non-nuclear end-users or non-nuclear end-uses, in North Korea will be considered on a case-by-case basis.

(ii) [Reserved]

(46) *Concealed object detection equipment described in ECCN 2A984*.

(i) *Syria*. Applications for all end-users in Syria of these commodities will generally be denied. Contract sanctity date: March 19, 2010.

(ii) *Sudan*. Applications for all end-users in Sudan of these commodities will generally be denied. Contract sanctity date: March 19, 2010.

(iii) *North Korea*. Applications for all end-users in North Korea of these commodities will generally be denied. Contract sanctity date: March 19, 2010.

(47) *“Software” described in ECCN 2D984 “required” for the “development”, “production” or “use” of concealed object detection equipment controlled by 2A984*.

(i) *Syria*. Applications for all end-users in Syria of these software will generally be denied. Contract sanctity date: March 19, 2010.

(ii) *Sudan*. Applications for all end-users in Sudan of these software will generally be denied. Contract sanctity date: March 19, 2010.

(iii) *North Korea*. Applications for all end-users in North Korea of these software will generally be denied. Contract sanctity date: March 19, 2010.

(48) *“Technology” described in ECCN 2E984 “required” for the “development”, “production” or “use” of concealed object detection equipment controlled by 2A984, or the “development” of “software” controlled by 2D984*.

(i) *Syria*. Applications for all end-users in Syria of these items will generally be denied. Contract sanctity date: March 19, 2010.

(ii) *Sudan*. Applications for all end-users in Sudan of these items will generally be denied. Contract sanctity date: March 19, 2010.

(iii) *North Korea*. Applications for all end-users in North Korea of these items will generally be denied. Contract sanctity date: March 19, 2010.

[69 FR 23630, Apr. 29, 2004, as amended at 69 FR 46076, July 30, 2004; 70 FR 14391, Mar. 22, 2005; 71 FR 20885, Apr. 24, 2006; 71 FR 51718, Aug. 31, 2006; 72 FR 20223, Apr. 24, 2007; 72 FR 62532, Nov. 5, 2007; 74 FR 2357, Jan. 15, 2009; 75 FR 14340, Mar. 25, 2010]

SUPPLEMENT NOS. 3–4 TO PART 742 [RESERVED]

SUPPLEMENT NO. 5 TO PART 742— ENCRYPTION REGISTRATION

Certain classification requests and self-classification reports for encryption items must be supported by an encryption registration, *i.e.*, the information as described in this Supplement, submitted as a support documentation attachment to an application in accordance with the procedures described in §§ 740.17(b), 740.17(d), 742.15(b), 748.1, 748.3 and Supplement No. 2 to part 748 of the EAR.

(1) Point of Contact Information

- (a) Contact Person
- (b) Telephone Number
- (c) Fax Number
- (d) E-mail address
- (e) Mailing Address

(2) Company Overview (approximately 100 words).

(3) Identify which of the following categories apply to your company’s technology/families of products:

- (a) Wireless
 - (i) 3G cellular
 - (ii) 4G cellular/WiMax/LTE
- (iii) Short-range wireless/WLAN
- (iv) Satellite
- (v) Radios
- (vi) Mobile communications, *n.e.s.*
- (b) Mobile applications
- (c) Computing platforms
- (d) Multimedia over IP
- (e) Trusted computing
- (f) Network infrastructure
- (g) Link layer encryption
- (h) Smartcards or other identity management

(i) Computer or network forensics

(j) Software

(i) Operating systems

(ii) Applications

(k) Toolkits/ASICs/components

(l) Information security including secure storage

(m) Gaming

(n) Cryptanalytic tools

(o) “Open cryptographic interface” (or other support for user-supplied or non-standard cryptography)

(p) Other (identify any not listed above)

(q) Not Applicable (Not a producer of encryption or information technology items)

(4) Describe whether the products incorporate or use proprietary, unpublished or non-standard cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body. (If unsure, please explain.)

(5) Will your company be exporting “encryption source code”?

(6) Do the products incorporate encryption components produced or furnished by non-